NUNAVUT INFORMATION AND PRIVACY COMMISSIONER

2007–2008 ANNUAL REPORT

Elaine Keenan Bengts
Information and Privacy Commissioner

NUNAVUT
INFORMATION
AND
PRIVACY
COMMISSIONER

5018 – 47th Street
P.O. Box 262
YELLOWKNIFE, NT
X1A 2N2

September 1, 2008

Legislative Assembly of Nunavut
P.O. Bag 1200
Iqaluit, NU
X0A 0H0

Attention: Honourable Peter Kilabuk
Speaker of the Legislative Assembly

Dear Sir:

I have the honour to submit my Annual Report as the Information and Privacy Commissioner of Nunavut to the Legislative Assembly for the period April 1, 2007 to March 31st, 2008.

Yours truly,

Elaine Keenan Bengts
Nunavut Information and Privacy Commission

In Yellowknife: 867-669-0976 ♦ Toll free: 888-521-7088 ♦ Fax: 867-920-2511 ♦ E-mail: ATIPPComm@theedge.ca

INDEX

	Page
Commissioner's Message	5
The Role and Mandate of the Information and Privacy Commissioner	14
Making and Access to Information Request	16
Protection of Privacy	17
The Request Process	18
Requests for Review	19
Review Recommendations Made	21
Review Recommendation 07-26	21
Review Recommendation 07-27	22
Review Recommendation 07-28	23
Review Recommendation 07-29	23
Review Recommendation 07-30	24
Review Recommendation 07-31	25
Review Recommendation 07-32	25
Review Recommendation 07-33	26
Review Recommendation 07-34	26
Review Recommendation 07-35	28
Review Recommendation 07-36	28
Review Recommendation 07-37	29
Review Recommendation 07-38	29

	Page
Review Recommendation 07-40	30
Review Recommendation 08-41	30
Review Recommendation 08-42	31
Looking Ahead	32
Privacy Reviews	32
Limitation Period for Requesting Reviews	33
Health Specific Privacy Legislation	34
Municipalities	35
Electronic Records Management	36
Security of Electronic Medium	37
Protecting Our Children	38
The Role of the Information and Privacy Commissioner	39

NUNAVUT INFORMATION AND PRIVACY COMMISSIONER

ANNUAL REPORT 2007-2008
2007—2008

COMMISSIONER'S MESSAGE

As Canadians, we must always question why our personal information is being collected whether by a government agency implementing a security program, or by a store employee compiling marketing data.

Jennifer Stoddart
Privacy Commissioner of Canada

In compiling the statistics for the year in preparation for the writing of this Annual Report, it became clear that 2007/2008 was by far the busiest year that I have had as Information and Privacy Commissioner, with 34 new files opened and 17 reviews completed. This is a positive thing, in my estimation, as it suggests that the public is becoming more aware of their rights under the Act and are using it for its intended purpose—to encourage open and accountable government.

As I write this Report, the world is awaiting the start of the 2008 Olympic Games in China. To me, the stories coming out of Beijing highlight the importance of being able to know what government is up to and to hold them responsible for their actions. Every day, it seems, news reports highlight what can happen when governments are not accountable. From the sometimes brutal repression of people's ability to challenge or even question government policy to invasive and ubiquitous monitoring and surveillance programs established by the Chinese government, we are reminded in a rather stark way of how different our way of life might be without the protections that we have in our systems of government. It re-enforces, to me, the importance of legislation such as the *Access to Information and Protection of Privacy Act*, particularly in today's technological world.

The Culture of Openness

Over the years, I have voiced a consistent message in my Annual Reports and in my reports to the Standing Committee on Government Operations—that there must be leadership from the top on access and privacy matters. This means that each and every elected official and every senior manager of every department and every public body should be knowledgeable

about the Act, its intents and purposes, and the general principals which underlie it. In my dealings with the various government departments, I sense that there is, for the most part, a commitment to the access provisions of the Act at all levels, even if the Act is not always applied consistently or fully. I sense a desire on the part of those involved in dealing with access requests, the ATIPP Co-ordinators, to do the right thing and to follow the spirit and intention of the Act. I commend the Government of Nunavut as a whole for their leadership in this regard and I would encourage all public bodies to continue to be diligent in maintaining that goal. This includes ensuring that there is ongoing training and that ATIPP Coordinators are given all of the resources and the time they need to deal with requests for information. Although it is unrealistic to suggest that there should be one employee solely dedicated to access and privacy issues within each public body, there are some departments, such as Health and Social Services and Education, which can reasonably be expected to require more of a time commitment to ATIPP matters than other departments. With a new Government coming in October, I would encourage all members of the new assembly to publicly and clearly endorse the purposes of the Act and to provide continued leadership in ensuring open government.

Protection of Privacy Needs More Attention

Although most public bodies are very diligent about access matters, I am somewhat more concerned about the attention being given to ensuring that personal information is protected and properly managed. It is very easy in the course of the day to day work of government to forget that the information being dealt with is sensitive and should be handled with care and respect. Although we have not yet had any reported incidents of data breaches in Nunavut, I have certainly seen the potential for that to happen. 2007 brought a record number of high profile cases across Canada and around the world involving serious data

> In an age characterized by revolutionary IT developments and exponential information creation, storage, transmission and use, the case for robust and credible information management has never been greater
>
> Ann Cavoukian
> 2007 Annual Report

Sadly in today's society one of your biggest worries will be how to keep your valuable IT equipment such as laptops, PDAs and iphones and the even more precious data they contain out of the hands of thieves. Laptop and mobile phone thefts from parked cars and conference rooms may grab headlines, but a far greater number of devices simply get left behind in cabs, on trains, and even on airplanes.

Becky Waring
PC Advisor (London, UK), February 2, 2008

breaches, many as a result of carelessness and lack of understanding about the importance of electronic data and other forms of records containing personal information. In the last few months there have been several incidents in both Saskatchewan and Alberta where sensitive medical records have been found in dumpsters and abandoned buildings, leaving thousands of people vulnerable not only to identity theft, but to having their medical histories seen by complete strangers. While there have been no formal complaints made to this office as of yet with respect to a "bulk" loss of personal information data, the potential for such a breach is very real. I have, for instance, heard of at least one incident of medical records being found in the dump at a small community in Nunavut. Furthermore, I would be surprised if there had not been incidents of lost or stolen computers, lap tops and PDAs containing sensitive personal information which simply have not come to my attention.

Quite apart from the statutory duty imposed on public bodies to protect personal information, a single high profile case can be devastating financially and result in a loss of public confidence. It has been estimated that for private industry, the average cost of a serious data leak is $1.8 million in direct and indirect costs. The cost to government would be no less and would come with a loss of confidence in the ability of government to manage not only information, but the economy.

Although human error will always be a factor that is difficult to control, there are steps that can be taken to reduce the possibility of data breaches. Vimal Vaidya, CEO at RedCannon Security, an IT security company that focuses on mobile devices, suggests six steps to minimizing the possibility of human error:

- There should be strong policies in place to define the acceptable uses of lap tops and PDAs and the kinds of information that can be stored on them
- Employees should be educated frequently and reminded of the rules of use
- There should be a centralized management of mobile devices, including

USB devices

- All data on mobile devices should be encrypted
- Steps should be taken to maintain control over USB ports
- There should be secure remote access to all electronic devices

But privacy breaches don't happen only as a result of lost or stolen mobile devices. Perhaps more widespread is simply the fact that often, when dealing with the day to day business of government, employees simply do not put their minds to the security and protection of personal information. Except perhaps in health services, where there are long standing and well established practices for the protection of personal information, many government agencies are more focused on "getting the job done" than on the privacy implications of what they do. More should be done in all public bodies to educate all employees of the importance of privacy and the security of personal information and the message should be frequent and consistent.

Electronic Health and Medical Records

One of the major challenges facing Nunavut, and all other Canadian jurisdictions, is in the health sector. I was very heartened to hear that the Department of Health and Social Services has taken steps to hire a full time employee to take the lead role on access and privacy matters. There is no doubt in my mind that with the race toward electronic health and medical records, and the difficult task of maintaining confidentiality in very small communities, this is a necessary step. As the country moves toward electronic health and medical records, there will be huge challenges to be met and overcome and Nunavut will have to deal with those challenges head on. The north-

> The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.
>
> United States Supreme Court Justice Louis Brandeis

ern territories, including Nunavut, may well have a greater burden in this regard than other parts of the country because we rely so heavily on services from other jurisdictions.

One of the projects I have been involved in this year is the Pan Canadian Forum on EHR Information Governance, sponsored by Canada Health Infoway. The Privacy Forum is intended to provide jurisdictions and oversight bodies with the opportunity to meet in a collegial setting in which they can share knowledge and experiences and can leverage their collective wisdom to facilitate the development of common solutions to common problems related to the information governance issues of the interoperable Electronic Health Record (EHR). Although there are many aspects to the EHR, health information privacy is definitely one of the most significant issues that my office is involved in and, without a doubt, the most complex. Every jurisdiction in Canada is dealing with these issues now, and the area promises to become far more complex before it resolves itself. The technical aspects of electronic health and medical records are beyond my expertise, although I am working hard to maintain a working understanding of the issues. It may be, however, that it is time to consider the possibility that the Office of the Information and Privacy Commissioner may have to engage the services of others with more specific and in depth knowledge of the issues on a contract basis to help to ensure that this office can keep up with the developments in the area.

> Information – especially personal information – is a core commodity in our digital era. Growth and success in the digital age depends, in part, on the extent to which the public trusts how personal information is collected, used, disclosed and retained by the organizations that hold it. There is a profound need for these organizations to manage personal information credibly. This requires not only adherence to fair information practices, but also intelligent technology choices
>
> Ann Cavoukian, Ontario Information and Privacy Commissioner
> 2007 Annual Report

I continue to encourage the Government of Nunavut to put their minds to creating health specific privacy legislation to guide us into the age of the electronic medical record. Virtually every other jurisdiction in Canada either has or is in the process of developing such legislation. Because Nunavut relies so heavily on the services of

other jurisdictions, I'm not sure that we can afford to ignore this issue for much longer without putting the people of Nunavut at a disadvantage in dealing with various health care providers. As the rest of the country moves toward the new electronic systems, Nunavut is going to have to keep pace so as to ensure that the people of Nunavut continue to enjoy the same level of protection with respect to their health records as those in other parts of the country.

Commissioners' Meetings

This year the Information and Privacy Commissioners issued two joint resolutions during their semi–annual meetings. The first, made in July, 2007 called on the Government of Canada to reconsider and revise the Passenger Protect Program (Canada's "no-fly" list) so as to ensure full public debate on the issues raised by the program and, in particular, the need for a formalized review mechanism so that those who think their names are on the list can challenge the inclusion. The resolution also called on the International Civilian Aviation Organization and the International Air Transport Association to defend and advance privacy principles, transparency and strong privacy protections in the establishment of any standards, rules or common practices governing the screening of travelers using watch lists or other passenger assessment programs.

The second joint resolution was issued in February, 2008 and addressed the concerns raised by Canada's Privacy Commissioners and Ombudsmen surrounding the development of Enhanced Drivers Licenses (EDL's) as a substitute identification document to the passport for travel between Canada and the United States. EDL's are being developed in a number of jurisdictions to meet the requirements of American authorities for identification documentation and contain Radio Frequency Identification Devices (RFID's) which contain electronic information about the holder. The Commissioners called on the Government of Canada and participating provinces and territories to ensure that no EDL project

> We need to make sure that somebody carries the can for failings in this area, and from that taking responsibility and changing the culture will follow. Personal information isn't sufficiently valued by organizations. The price of this is people losing trust in public services. Trust relies on respecting people's personal information, and data protection is about more than security, it's about informing people how their information is used and about minimizing the amount.
>
> David Smith
> United Kingdom Deputy Information Commissioner

proceeds on a permanent basis unless the personal information of participating drivers remains in Canada. The resolution further called on the federal and provincial/ territorial governments to ensure that the personal information stored on or in the EDL can be accessed only by the Customs and Border Protection and can be used only for the purpose of determining whether an individual is eligible for admission to the United States.

I was also privileged this year to be able to attend the 29th International Conference of Data Protection and Privacy Commissioners held in Montreal in September, 2007 as an accredited member of that organization and to hear some of the world's foremost authorities on privacy issues address some of the most significant issues of our day. This conference, held annually, brings together 78 data protection authorities and privacy commissioners from every continent. The public sessions included speakers such as Mr. Simon Davies, the President of Privacy International (UK), Dr. Michael Geist, Canadian Research Chair in Internet and E-Commerce Law, University of Ottawa, and Dr. Bradley A. Malin, Assistant Professor, Department of Biomedical Infomatics, Vanderbilt University (USA) on issues ranging from children's on-line privacy to nanotechnology. In a closed session, the representatives of the accredited authorities had the opportunity to exchange information about their organizations and adopt resolutions in fields which pose common challenges. There were two significant resolutions passed at the 2007 conference — a resolution on the urgent need for global standards for safeguarding passenger data to be used by governments for law enforcement and border security purposes and a Declaration of Civil Society Organizations on the Role of Data Protection and Privacy Commissioners.

> Gaining access to information, participating in discussions and debates and thereby enjoying the guaranteed purpose under the freedom of information and protection of privacy legislation – this is just the first step towards ensuring real equality for all Nova Scotians and to achieve the goal of participatory democracy.
>
> Dulcie McCallum,
> Nova Scotia Access to Information Review Officer

Priorities for the Next Year

I have two priorities for the coming year. One is to bring some prominence to the Right to Know Week, during the Week of September 29 to October 3, 2008. The second is to focus some attention on children's on-line privacy and the role that the internet plays in the lives of our children.

The purpose of Right to Know Week is to raise citizen awareness about their right to access information under the control of government institutions. In 2008 Canadian Right to Know Week will take place from September 29th to October 3rd.

This year marks the third year that Canadians have celebrated Right to Know Week, and there are a great number of events planned all across Canada. Internationally, Right to Know Day began in Sofia, Bulgaria at an international meeting of access to information advocates who proposed that a day be dedicated to the promotion of freedom of information worldwide. Right Know Day is now celebrated annually by over 60 different countries on September 28th. During that week I will be launching an essay competition for all high school students in Nunavut and will be drawing on the resources of my colleagues from other parts of the country to raise the profile of the access to information provisions of the Act.

The second issue I would like to spend some time addressing in the next year is how to help our children learn more about how to protect themselves on the internet. In an article entitled "Virtual Playgrounds and BuddyBots: A Data-minefield for Tweens" by Valerie Steeves and Ian Kerr which was published in the Canadian Journal of Law and Technology in 2005, they say:

> The online world of tweens - kids between the ages of nine and 14 - is fun, interactive, and cool. It is also a place that is structured by seamless surveillance and the aggressive collection of children's personal information.

> From a child's point of view this boundary between the real world and the online world is becoming increasingly meaningless.
>
> Valerie Steeves
> Associate Professor, Department of Criminology, University of Ottawa in address to the Terra Incognita Conference, Montreal, September 2007 on Childrens' Online Privacy

...society has come to realize that privacy is at the heart of liberty in a modern state....Grounded in a man's physical and moral autonomy, privacy is essential for the well being of the individual

R. v. Dyment [1988] 2 S.C.R. 417 at 427-428, 55 D.L.R. (4th) 503 at 513

> Whether kids are hanging out with Hilary Duff on Barbie.com, playing with Lifesaver products on Candystand, or chatting with ELLEgirlBuddy about their favorite celebrities, a marketer is listening - and sometimes talking - to them, to measure their likes, dislikes, aspirations, desires, wishes, and propensity to purchase product

Over the course of the last year, I have started to learn much more about the dynamic between our children and the internet and the significant role that it plays in their lives. Canada is one of the most "wired" countries in the world, with almost 90% of households having at least one computer with internet access. Our children are leaving their parents far behind in their understanding and abilities to access the on-line world. Who is teaching these children about how to protect themselves on the internet, from predators and from identity theft? Who is teaching them about why it is important to protect their personal information? Recent studies suggest that while most children have a basic understanding of the most obvious dangers of giving out their personal information on one, there are huge gaps in their appreciation of the serious consequences that might result from giving away too much personal information. Because the internet is so much a part of youth culture, it is important that they have an understanding of the ways that they can be affected. I am , therefore working on some projects to assist teachers and parents to help Nunavut children to be more aware of the how they use the internet and what kind of information they share.

THE ROLE AND MANDATE OF THE INFORMATION AND PRIVACY COMMISSIONER

Nunavut's *Access to Information and Protection of Privacy Act (ATIPPA)* came into effect prior to division on December 31st, 1996. When Nunavut was created, the Act became part of the law of Nunavut. It binds all Territorial Government departments and agencies and establishes the rules about how Territorial government agencies collect, use and disclose personal information and about how the public can gain access to government records. Under the Act, the office of the Information and Privacy Commissioner (IPC) is created. The IPC is an officer of the Legislature and is appointed by the Commissioner of Nunavut on the recommendation of the Legislative Assembly. She reports to the Legislative Assembly of Nunavut. The IPC is an independent officer and can be only be removed from office "for cause or incapacity" on the recommendation of the Legislature.

The term "access to information" refers to the right of the public to have access to general records relating to the activities of government, ranging from administration and operations to legislation and policy. It is an important aspect of open and accountable government. Under the *Access to Information and Protection of Privacy Act,* the public is given the right to have access to all "records" in the possession or control of a public body through an access to information request, unless the record is subject to a specific exemption from disclosure as provided for in the Act. The exceptions to the open disclosure rule function to protect individual privacy rights, allow elected representatives to research and develop policy and the government to run the "business" of government.

> The "overarching purpose of access to information legislation [...] is to facilitate democracy." The legislation does this by insuring that citizens are properly informed so as to be able to participate meaningfully in the democratic process and by insuring that politicians and bureaucrats remain accountable to citizens.
>
> Dawson J., A.G. Canada v. Information Commissioner of Canada; 2004 FC 431, [22])

The Supreme Court of Canada has clearly stated that exemptions to disclosure pro-

vided for in access to information legislation should be narrowly interpreted so as to allow the greatest possible access to government records.

The Act also gives individuals the right to see and make corrections to information about themselves in the possession of a government body.

Privacy protection is the other side of that equation, and refers to the safeguarding of personal information held by government.

ATIPPA applies to all government departments and most agencies, boards and commissions established by the government.

The Information and Privacy Commissioner has several roles under the Act, including:

- independently reviewing the decisions and practices of government organizations concerning access and privacy and providing recommendations to public bodies with respect to those issues
- providing comment and advice on proposed government legislation and programs;
- educating the public about the Act

When dealing with access to information issues, the Information and Privacy Commissioner has very limited power to make binding orders with respect to matters which come before her. Rather, in most cases her role is similar to that of an Ombudsman. Recommendations are made to the head of the public body involved who must then make a final decision as to how the government will deal with the matter. If, in the end, the person seeking the information is still not satisfied with the response received, there is recourse to the Nunavut Court of Justice for a final determination of the matter.

> The essence of liberty in a democratic society is the right of individuals to autonomy – to be free from state interference. The right to privacy has several components, including the right (with only limited and clearly justified exceptions) to control access to and the use of information about individuals. Although privacy is essential to individual autonomy, it is not just an individual right. A sphere of privacy enables us to fulfill our roles as community members and is ultimately essential to the health of our democracy.
>
> Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing; B.C. OIPC, Oct. 2004, p. 13)

MAKING AN ACCESS TO INFORMATION REQUEST

Requests for information must be made in writing and delivered to the public body from whom the information is sought. Although forms are available, requests for information do not need to be in any particular form. The only requirement is that the request be in writing. This would include a request made by e-mail but where a request is made by e-mail, it may not be considered complete until the public body receives confirmation of the request with the applicant's signature. Requests for information are subject to a $25.00 application fee except in cases where the information requested is the applicant's own personal information. In such cases, there is no application fee, although there may be a fee for copying records in certain circumstances.

When a request for information is received, the public body has a duty to identify all of the records which are responsive to the request and to respond to the request within 30 days. Once all of the responsive documents are identified, they are reviewed to determine if there are any records or parts of records which should not be disclosed for some reason. The public body must endeavor to provide the applicant with as much of the requested information as possible, while at the same time respecting the limited exceptions to disclosure specified in the Act. Public Bodies are prohibited from disclosing certain kinds of records. In some instances, the Public Body has discretion to decide to either disclose the records or not. These discretionary exemptions require the public body to consider whether or not to

> One of the fundamental contrasts between free democratic societies and totalitarian systems is that the totalitarian government relies on secrecy for the regime but high surveillance and disclosure for all other groups, whereas in the civic culture of liberal democracy, the position is approximately the reverse
>
> Professor Geoffrey de Q Walker, Dean of Law at Queensland University.

disclose the information, keeping in mind the purposes of the Act and the weight of court authority which requires public bodies to err on the side of disclosure.

Every person has the right to ask for information about themselves. If an individual finds information on a government record which they feel is misleading or incorrect, a request in writing may be made to correct the error. Even if the public body does not agree to change the information, a notation must be made on the file that the individual has requested a correction.

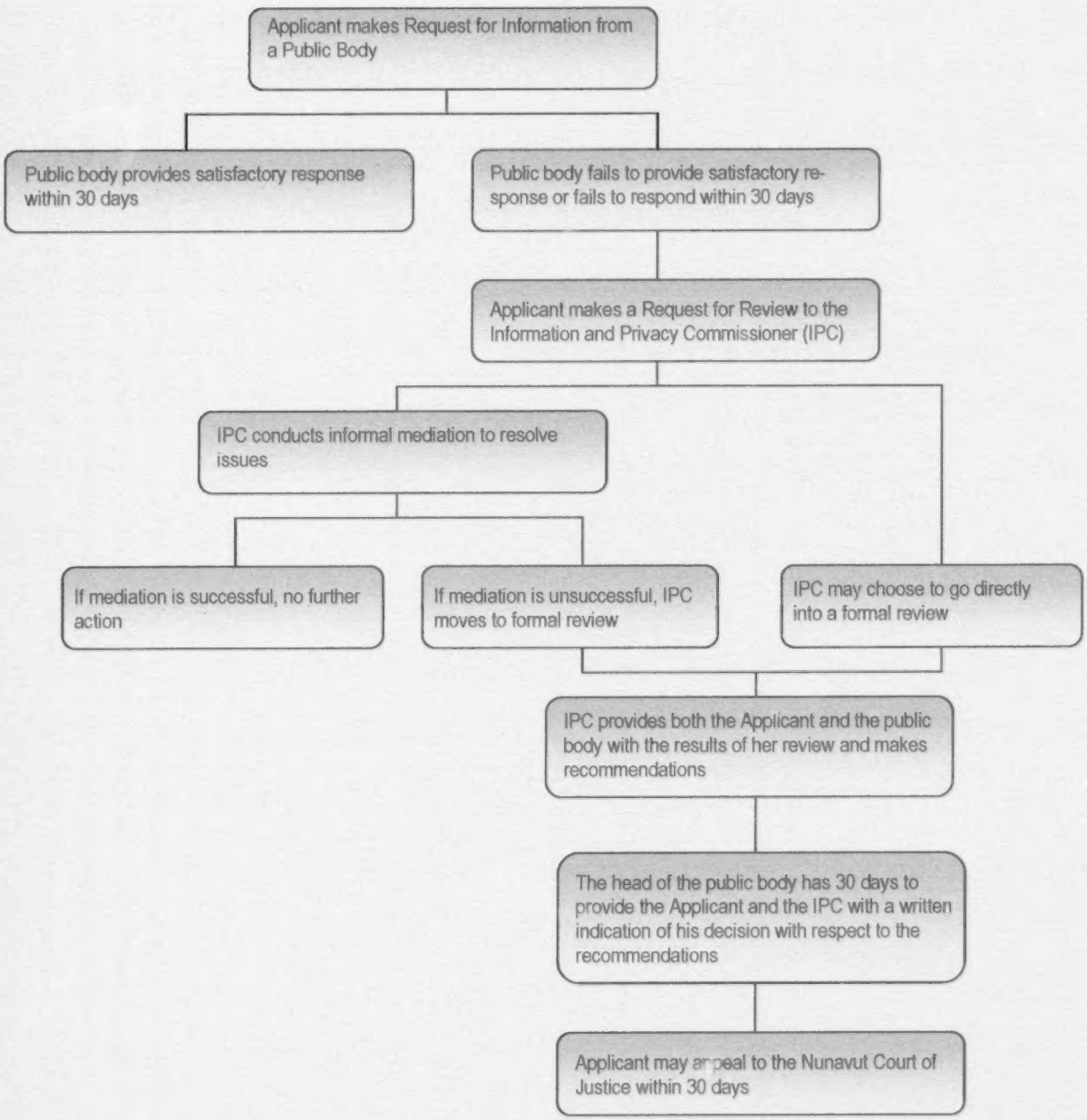
> At its root, I feel the best privacy protection is grounded in attitude — an attitude which should flow naturally from an appreciation of the nature of the relationship between government and members of the public. Governments exist at the pleasure of the governed — and privacy protection is an essential part of the relationship.
>
> A Special Report to the Legislative Assembly of Ontario on the Disclosure of Personal Information at the Ministry of Health
> Submitted by Tom Wright
> Former Information and Privacy Commissioner/Ontario

PROTECTION OF PRIVACY

Part II of the *Access to Information and Protection of Privacy Act* sets out the rules about how public bodies can collect personal information, how they can use it once it has been collected and how and when they can disclose it to others. The Act also requires public bodies to ensure that they maintain adequate security measures to ensure that the personal information which they collect cannot be accessed by unauthorized personnel. This Part of the Act also provides the mechanism for individuals to be able to ask the government to make corrections to their own personal information when they believe that an error has been made.

As of yet, the Information and Privacy Commissioner has no legislated role in the review of complaints made by members of the public who feel that their personal information has been improperly collected, used or disclosed by a public body. Notwithstanding this lack of legislated authority, the Information and Privacy Commissioner will accept privacy complaints and will attempt to address the concerns of individuals in this situation.

THE REQUEST PROCESS


Applicant makes Request for Information from a Public Body
Public body provides satisfactory response within 30 days
Public body fails to provide satisfactory response or fails to respond within 30 days
Applicant makes a Request for Review to the Information and Privacy Commissioner (IPC)
IPC conducts informal mediation to resolve issues
If mediation is successful, no further action
If mediation is unsuccessful, IPC moves to formal review
IPC may choose to go directly into a formal review
IPC provides both the Applicant and the public body with the results of her review and makes recommendations
The head of the public body has 30 days to provide the Applicant and the IPC with a written indication of his decision with respect to the recommendations
Applicant may appeal to the Nunavut Court of Justice within 30 days

REQUESTS FOR REVIEW

Under section 28 of the Access to Information and Protection of Privacy Act, a person who has requested information from a public body, or a third party who may be affected by the disclosure of information by a public body, may apply to the Information and Privacy Commissioner for a review of the public body's response to a request for information. This includes decisions about the disclosure of records, corrections to personal information, time extensions and fees. The purpose of this process is to ensure an impartial avenue for review and independent oversight of discretionary and other decisions made under the Act.

A Request for Review must be made in writing to the Information and Privacy Commissioner's Office within 30 days of receiving a decision from a public body under the Act. There is no fee for a Request for Review.

When the Information and Privacy Commissioner receives a Request for Review, she will take steps to determine what records are involved and obtain an explanation from the public body. In most cases, the Commissioner will receive a copy of the responsive documents from the public body involved and will review the records in dispute. In some cases, it may be necessary for the Information and Privacy Commissioner to attend the government office to physically examine the public body's files. Generally, an attempt will first be made by the Commissioner's Office to mediate a solution satisfactory to all of the parties. In several cases, this has been sufficient to satisfy the parties. If, however, a mediated resolution does not appear to be possible, the matter moves into a more in depth review. All of the parties involved, including the public body, are given the opportunity to make written submissions on the issues.

In the 2006/2007 fiscal year, the Informa-

There is no magic solution to the shortcomings of the system. A healthy access to information system needs:

- All its parts functioning well in order to deliver the outcomes intended by parliament
  - The right systems to process requests
  - Skilled staff
  - Supportive managers and Ministers
  - Adequate resources
  - Good information management
  - Good understanding of the principles and the rules by all, including third parties
  - And effective approaches to oversight.

2002 Delagrave Report

tion and Privacy Commissioner's Office opened thirty five files.

- Requests for Review (Access) 17
- Requests for Review (Fees) 2
- Requests for Review (Privacy) 1
- Requests for Comment 2
- Request to Lay Charge (s. 59) 7
- Request for Correction to Personal Information 1
- Other 5

Only four public bodies were involved in the Requests for Review as follows:

- Education 15
- Health and Social Services 4
- Human Resources 6
- Community and Government Services 3

The Information and Privacy Commissioner issued sixteen Review Recommendations in 2006/2007, up from two in 2007/2008.

Two Requests for Review were considered abandoned when the IPC did not receive a response to her request for further details about the issues raised. In addition, one matter was judged by the IPC to be premature and sent it back to the applicant with suggestions as to the proper way to proceed.

In one case, the IPC exercised her discretion pursuant to Section 31 (2) and refused to conduct a review. In that case the Applicant asked the IPC to review the public body's failure to respond to a Request for Information within 30 days when it was clear that by the time the Request for Review was made, the response had been received. The IPC found, in the circumstances, that the Request for Review concerned a trivial matter and need not be completed to ensure that the objectives of the Act were maintained.

There were seven requests, all from the same Applicant, that the IPC lay a charge against a public body pursuant to Section 59(2) of the Act, which makes it an offence to obstruct the IPC in the exercise of the performance of her duties under the Act, fails to comply with a request from the IPC, or makes a false statement to the IPC. The IPC declined to lay any charges or to consider any further such requests from the Applicant.

There were two requests to the Information and Privacy Commissioner to provide input and comments on proposed legislation, and those requests were with respect to the Official Languages Act and amendments to the Access to Information and Protection of Privacy Act.

REVIEW RECOMMENDATIONS MADE

Review Recommendation 07-26

This review arose out of a complaint by an individual who felt that her personal health information had been improperly accessed and disclosed without her consent. The complainant was concerned that an employee of the health centre in the community in which she lived had disclosed details about her medical situation to her former spouse, with whom she was engaged in legal proceedings. She was also concerned about hand written notations on "sticky notes" which she had seen on her medical file.

The health centre could not verify definitively that its employee did not have access to the complainant's file, nor could they verify that the employee had not passed on any information on the file to a third party. They relied, instead, on the policies they had in place and relied on the professionalism of the employee.

The Information and Privacy Commissioner concluded that it was, in fact, not possible to determine whether or not the Complainant's health record was inappropriately accessed or disclosed. She did, however, point out that the existence of strong policies, by themselves, do not guarantee that they will be followed. A number of recommendations were made to the Department of Health and Social Services to review and revise policies and to ensure that all employees are reminded of their duties and responsibilities under the *Access to Information and Protection of Privacy Act* to ensure compliance.

The public body received the recommendations made and agreed to consider them as they moved forward to minimize the possibility of inappropriate disclosures in the future.

> While the hospital had policies in place to safeguard health information, they were not followed completely, nor were they sufficient to prevent a breach ... from occurring. In addition, the fact that the nurse chose to disregard not only the hospital's policies but her ethical obligations as a registered nurse ... disregarding three warnings alerting her to the seriousness of her unauthorized access, is especially troubling. Precautions against such blatant disregard for a patient's privacy by an employee of a hospital must be built into the policies and practices of a health institution.
>
> Ontario Information and Privacy Commissioner
> Order HO-002

Review Recommendation 07-27

In this case, the Applicant submitted a Request for Information to the Department of Education and he alleged that the public body had not responded to the request within 30 days as required, resulting in a "deemed refusal" to provide the information requested.

Upon review of the matter, it appeared that the Request for Information had been made on June 19th. A letter dated June 28th was sent to the Applicant imposing an extension of time to respond, as is allowed under section 11 of the Act. The deadline for response was extended to August 2nd. It is unclear when the letter was posted to the Applicant or when it was received by him.

The Information and Privacy Commissioner determined that an extension of time properly taken under section 11 of the Act and communicated to the Applicant is a sufficient "response" to prevent a finding of "deemed refusal" under the Act, provided that the extension of time is communicated to the Applicant within the initial 30 days. She further determined that although public bodies should always endeavor to have responses actually delivered into the hands of an Applicant within 30 days, it is sufficient if the letter is postmarked within 30 days because the public body has no control over delays in the post office or delays by the Applicant in picking up his mail.

The Recommendations made were accepted by the public body.

> In my opinion, the Act requires only that the public body have "responded" in writing within the 30 days and sent that response by some reasonable means in order to have "responded" within 30 days. Otherwise, the legislation would have specifically stated that the public body was required to "deliver" its response within 30 days. In this case, the letter was put in the mail more than 20 days ahead of their deadline. Once placed in the mail, there is no control over how long it might take to be delivered to the Applicant.
>
> Review Recommendation 07-27

Review Recommendation 07-28

The Applicant made a Request for Information from the Department of Education for certain documents. Before the public body would complete the request, they advised the Applicant that he would have to pay the $25.00 application fee. The Applicant objected to the payment of the fee as it was his position that the information requested was his own personal information and he was entitled to receive it without paying the fee.

After reviewing the responsive records, the Information and Privacy Commissioner (IPC) found that the information requested did contain some personal information of the Applicant but was not limited to his own personal information and that the public body was justified in requesting the payment of the $25.00 application fee. She further suggested, however, that more care should be taken when responding to Applicants to ensure that there is no confusion about when a fee is applicable.

The Recommendations made were accepted by the public body.

Review Recommendation 07-29

This was another in a series of Requests for Review received in which there was an allegation that the public body had not responded to the Request for Information within 30 days and there was, therefore, a deemed refusal to respond.

In this case, the IPC determined that the public body had responded to the Applicant's Request within 30 days by extending the time to respond pursuant to section 11 of the Act Several recommendations were made, however, to avoid similar situations arising in the future, including the suggestion that extension letters be sent by fax where the Applicant has provided a private facsimile number, the possibility of advising the Applicant by telephone that an extension letter has been sent, and sending correspondence to Applicants by means of delivery that can be traced in terms of dates sent and received.

The Recommendations were accepted by the public body

Disclosure of the names and titles of employees, acting in their formal representative capacities, is generally not an unreasonable invasion of their personal privacy

Order F2006-008 at paras. 42 and 46
Alberta Information and Privacy Commissioner

Review Recommendation 07-30

In this case, the Applicant was objecting to the fees levied by the Department of Human Resources on the Applicant's Request for Information. The department had estimated photocopying costs of $40 and requested payment of half of that amount before they would proceed with the request. The Applicant's position was that the assessment of photocopying fees was discretionary and that they should, in his case be waived because he was broke and destitute because he had lost his job. Furthermore, he felt that there was significant public interest in the disclosure of the records requested because, in his view, their disclosure would reveal illegal or improper activities by government employees and union representatives.

The public body pointed out that although the regulations under the Act allowed for a waiver of fees upon a request to the head of the public body, the granting of a waiver is discretionary and the Applicant in this case did not make any such application to the public body but brought the matter directly to the IPC. They also pointed out that the estimated fees assessed in this case were approximately half of the actual final cost associated with responding to the request.

The IPC agreed that the ability to waive fees was discretionary on the part of a public body and that she had no jurisdiction to interfere with the exercise of that discretion, provided that it was clear that the discretion had, in fact, been exercised. In this case she was satisfied that the public body had weighed the pros and cons of imposing the fee and that the department had, as a result, complied with the Act when assessing the fee. The IPC recommended that the fee assessment stand.

The Recommendation was accepted.

> In particular, I wish to be a strong advocate for the duty of all federal institutions to help in any way they can the individuals and organizations who request information from them to get that information.
>
> Robert Marleau
> Information and Privacy Commissioner for Canada
> Annual Report 2007/2008

Another important theme emerging from the past year is the apparent lack of awareness on the part of many public bodies and organizations of the weaknesses in their technical and administrative information security. This is bad for privacy. It is also bad news for the security of corporate or government information assets.

David Loukidelis
Information and Privacy Commissioner of B.C.
2007/2008 Annual Report

Review Recommendation 07-31

This was another case in which the IPC was asked to determine whether the public body had responded to a Request for Information within the allotted 30 days. The Request for Information had originally been submitted to the Department of Community and Government Services but was transferred to the Department of Human Resources as the public body most likely to have the information requested.

A letter was sent to the Applicant extending the time for responding to the request pursuant to section 11 of the Act. The public body provided tracking information from Canada Post indicating that the response had been posted well in advance of the 30 day deadline and was available for pick up by the Applicant prior to the deadline as well but that it was not actually retrieved by him until after the 30 days.

The IPC found that the public body had responded with 30 days and her only recommendations were aimed at improving the process to avoid similar problems again.

The recommendations were accepted.

Review Recommendation 07-32

The Applicant in this case was seeking a correction to his personal information. There was, once again, an allegation that the public body had not responded to that request within the requisite 30 days resulting in a deemed refusal to make the correction.

Once again the IPC found that the public body had responded within the 30 day period by posting a letter to the Applicant within the 30 days extending the time for response. The requested correction was made within the extended period of time.

In this case, the IPC raised some concerns about the extension of time and questioned its *bona fides*. She was not satisfied that any of the allowable reasons for the extension existed. That aside, she noted that the requested correction had been made thereafter and there was, therefore, no need to make any further recommendations .

The report and recommendations were accepted.

Review Recommendation 07-33

This matter arose out of a Request for Information originally made to the Department of Community and Government Services but transferred to the Department of Human Resources for response. The complaint in this case was, once again, that the public body did not respond within the 30 day response period, resulting in a deemed refusal to disclose the information requested.

In this case the public body was able to provide me with tracking records from Canada Post indicating that a letter extending the time for responding to the application had been posted prior to the end of the 30 day response period but had not been delivered within 30 days.

Again the IPC found that the public body had, in fact, responded within the time allotted and there was no deemed refusal .

The Recommendations made were accepted.

Review Recommendation 07-34

The Applicant in this case requested a copy of correspondence allegedly sent to certain third parties as a result of an investigation conducted by the Department of Health and Social Services concerning the welfare of a child.

In their first response to the Applicant, the public body indicated that there were no responsive records. The Applicant, however, produced correspondence he had received several years earlier indicating that there was, in fact, a file dealing with the incident. After receiving the additional information included by the Applicant in his Request for Review, the public body did further searches and found the file in question. They refused to disclose any part of it, however, on the basis that the records formed part of a child welfare file pursuant to the *Child and Family Services Act* and that disclosure of such records was prohibited. They also indicated that, even though

> The access provisions of the Freedom of Information and Protection of Privacy Act are not harsh in terms of what has to be disclosed: there are ample exceptions to disclosure which protect specific interests of public bodies. Leadership is everything: if the head of the public body upholds openness, that will influence the entire organization.
>
> Frank Work
> Information and Privacy Commissioner of Alberta
> 2007 Annual Report

In Canada, Right to Know Week is celebrated to promote the right to information as a fundamental human right and to campaign for citizen participation in open, democratic government. This national event offers an opportunity for anyone interested in promoting freedom of information as a fundamental right to engage in an informed dialogue with Canadians of all ages.

Robert Marleau
Information Commissioner for Canada
Annual Report 2007/2008

they had found the file, there was no record matching the description of the one requested by the Applicant.

The IPC agreed with the public body's assessment that the file in question was exempt from disclosure pursuant to section 71 of the *Child and Family Services Act* which prohibits the disclosure of information contained in a child welfare file, notwithstanding the provisions of the *Access to Information and Protection of Privacy Act*.

In this case, however, the IPC expressed concerns that the records requested had not been discovered in the first instance and that the circumstances suggested that there might be a problem with the record keeping system, as opposed to the efforts made by the public body to locate the records. She pointed out that there was really no new information contained in the Request for Review that had not been provided by the Applicant in his original Request for Information. She therefore recommended that the public body investigate why the records in question did not surface during the initial attempt to find them and to correct any problems with the records management system that might come to light as a result of that investigation.

It appears that the public body did, in fact, review the procedures followed in attempting to locate the records requested but could find no specific errors in the steps taken. They further stated in their response to the recommendations made that they were confident that the Department of Health and Social Services is managing the records management system in a responsible and conscientious manner.

Review Recommendation 07-35

This case raised identical issues as the issues in Review Recommendation 07-34. The only difference was that the Applicant was asking for access to a different record. The same recommendations were made and the same response was received from the public body.

ing a more complex search of a large number of records. The Applicant took the position that the absence of the named individuals should have no effect on the time necessary to compile the records unless they had not been managed in accordance with government standards and practices.

In its response to the Request for Review, the public body provided the IPC with a more detailed explanation for the need for the extension, indicating that the absence

> The most common cause of disputes, in the information and privacy world as in any other dealings between ordinary citizens and organizations, is communication breakdowns that have little to do with legal rights or obligations.
>
> David Loukidelis
> Information and Privacy Commissioner of BC
> Annual Report 2007/2008

Review Recommendation 07-36

The Applicant in this case asked me to review the extension of time which the public body had taken to respond to his Request for Information. In its letter to the Applicant advising him of the extension, they advised him that they required the extension because some or all of the individuals named in the Request for Information were no longer employed in the positions held at the time the records were created, necessitat-

of the individual employees named in the Request for Information necessitated both electronic searching of those peoples' stored electronic files and a physical search of records storage locations. This increased both the number of searches necessary and the volume of records that needed to be reviewed to determine if they were responsive. Furthermore, they pointed out that the request was made during the summer months when the Depart-

ment personnel is often depleted so that those employees most able to advise where to find the specific records requested might be found are not available.

The IPC found that the public body had a legitimate reason for the extension of time to respond but did not do a good job in articulating those reasons to the Applicant. She made recommendations with respect to the wording of the letter sent to Applicants in such situations.

The Recommendations were accepted.

Review Recommendation 07-38

This case raised identical issues as the issues in Review Recommendation 07-36. The only difference was that the Applicant was asking for access to different records. The same recommendations were made and the same response was received from the public body.

> The spontaneous nature of e-mail leads to the creation of records containing information that in the past would never have been committed to paper. Such information is often quite sensational to applicants, particularly journalists, who routinely seek out this type of "juicy" information.
>
> Sandy Hounsel
> Assistant Information and Privacy Commissioner
> of Newfoundland and Labrador
> Electronic Records and Access to Information

Review Recommendation 07-37

This case raised identical issues as the issues in Review Recommendation 07-36. The only difference was that the Applicant was asking for access to different records. The same recommendations were made and the same response was received from the public body.

Review Recommendation 07-39

This case raised identical issues as the issues in Review Recommendation 07-36. The only difference was that the Applicant was asking for access to different records. The same recommendations were made and the same response was received from the public body.

Review Recommendation 07-40

The issue here was, once again, the question of whether or not the public body, in this case the Department of Community and Government Services, had responded to the Applicant's Request for Information within the 30 days provided for.

In this case, by providing tracking information from Canada Post, the public body was able to demonstrate not only that they had responded on a timely basis, but that response was, in fact received by the Applicant within the 30 day period. The IPC recommended that no further action be taken.

The recommendations were accepted.

Review Recommendation 08-41

The Applicant requested "individual level data" from the Nunavut Cancer Registry. Although he did not identify himself as such, it appeared from the nature of the request that he was a researcher and was asking for the information for the purposes of his research project. Specifically, the Applicant was asking for a computerized file of data that contained records of each person diagnosed with cancer in Nunavut for the whole period for which cancer incidence data were available. Although he did not want names, health numbers or social insurance numbers, he did ask for information such as year of diagnosis, age at diagnosis, gender, ethnicity, residence, type of cancer and follow up treatment. The public body denied access to the records based not on the provisions of the *Access to Information and Protection of Privacy Act,* but on the limitations set out in the *"Disease Registries Act"* which they felt took precedence over ATIPPA.

The IPC concluded that both Acts prohibited the disclosure of the requested information in the circumstances of this request and recommended that no further action be taken.

The recommendations were accepted.

In other words – as users are often warned, but as many refuse to believe – sending an unencrypted e-mail is the equivalent of writing a message on the back of a postcard. Anyone through whose hands it passes – or anyone nosy enough to crane their neck and look – can read such a message without violating the presumed right to privacy of either the sender or the recipient, because when they presume privacy, they simply presume wrong.

NewsFactor Network, August 13, 2008

> The language in the Access to Information and Protection of Privacy Act, like other access and privacy statutes in Canada, creates a bias in favour of disclosure. By providing a specific right of access and by making that right subject only to limited and specific exceptions, the legislature has imposed a positive obligation on public bodies to release information, unless they are able to demonstrate a clear and legitimate reason for withholding it. Furthermore, the legislation places the burden squarely on the head of a public body that any information that is withheld is done so appropriately and in accordance with the legislation.
>
> NL OIPC Report 2005-002

Review Recommendation 08-42

In this case, the Applicant was requesting a copy of a report which was prepared in connection with an investigation into an allegation of workplace harassment, as well as all the background materials in relation to the preparation of the report. The public body had provided a number of records, but some were edited and access to others was refused. In most cases, the reasons given for the edits were that the severed portions constituted the personal information of third parties that was either:

- compiled and was identifiable as part of an investigation into a possible contravention of law, or
- that the disclosure could reasonably be expected to reveal that the third party supplied, in confidence, a personal recommendation or evaluation.

The IPC reviewed each severance and made recommendations with respect to each one.

The IPC also, however, chastised the public body for its indiscriminate and poorly applied use of the discretionary exemptions without much thought. She reminded the department that disclosure was the rule, and that the onus of establishing that an exemption applied lay with the public body. With that in mind, the public body's explanations did not contain enough background about the creation of the record or its contents to give the IPC enough information on which she could find that the onus was met. She encouraged the public body, when exercising its discretion to refuse disclosure in these matters to take the responsibility of exercising that discretion seriously and to actively consider both the pros and the cons of such disclosure keeping in mind the over-riding objective of the Act was to allow disclosure.

The majority of the many recommendations made in this case were accepted.

LOOKING AHEAD

There is always room to improve any system and this holds true as well for access and privacy. Some of the recommendations which follow have been made before. With respect to those, I would urge the Government of Nunavut to take steps to address them in some fashion or another. Some of the recommendations being made would require amendments or revisions to the *Access to Information and Protection of Privacy Act*. It may be that the time has come for a more comprehensive review of the Act to ensure that it keeps up with the challenges of access and privacy in a wired world.

> We're waking up in a surveillance society. And when you start to see how many well-intentioned, apparently beneficial schemes are in place to monitor people's activities and movements, I think that does raise concerns. It can stigmatize people. I have worries about technology being used to identify classes of people who present some sort of risk to society. And I think there are real anxieties about that.
>
> Richard Thomas
> UK Information Commissioner

Privacy Reviews

As pointed out in previous years, although the *Access to Information and Protection of Privacy Act* outlines rules and regulations with respect how government can collect, use and disclose personal information, nothing in the Act provides a mechanism to enforce or monitor those rules. The only provision which deals with breaches of the privacy provisions of the Act is Section 59 (1) which provides that any person who knowingly collects, uses or discloses personal information in contravention of the Act or the regulations is guilty of an offence punishable on summary conviction and liable to a fine not exceeding $5,000. This is inadequate to adequately protect privacy for a number of reasons. Firstly, it contemplates that the offender "knowingly" collects, uses or discloses personal information in contravention of the Act. It is my experience that most privacy breaches are inadvertent or occur because not enough thought has gone into the matter, rather than through an intentional act. Secondly, it requires someone to take the step of having a charge laid under the act and prose-

cuted by someone. That is unlikely to happen except in most egregious of circumstances. Thirdly, fining someone for contravening the Act will not result in any changes that could prevent similar problems down the line.

What is needed is a way to catch imperfections in the system and address them. It seems to me that a formal independent oversight function could address this issue and allow members of the public who feel that their personal information has been collected, used or disclosed contrary to the Act a way to address their concerns in a more effective way. Although I do informal reviews and make informal recommendations, there is currently no obligation imposed on public bodies to co-operate with my investigations or to take an steps to address recommendations made.

This is a recurring recommendation and one that needs to be addressed to ensure that the people of Nunavut continue to have the same level of privacy protection as most other Canadians.

Limitation Period for Requesting Reviews

The Act as it is currently worded allows an Applicant only thirty days after receiving a response to a Request for Information to ask the Information and Privacy Commissioner to review that decision. This is really a very short time frame when one takes into consideration the often slow delivery of conventional mail and the fact that people do not always have fax machines or computers at their disposal. There have been numerous instances in which the Request for Review has been received in my office a day or two after the end of the 30 day period. Because the Act does not give the Information and Privacy Commissioner any jurisdiction to review a request made after the deadline, or to extend the time where appropriate, the Request for Review cannot proceed. In a number of cases, I have asked the public body to agree to allow the review to proceed in any event and the public bodies have complied with those requests because the alternative is to send

---

People expect, and are entitled to expect, that the government will not share their confidential or personal information without their consent.

Cheskes v. Ontario (Attorney General)
2007 CanLII 38387 (Ont. Sup. Ct)
Justice Edward Belobaba

---

the Applicant back to make the same request a second time, presumably get the same response as the first time and seek a review in a more timely fashion the second time. The only instance in which a limitation period for asking for a Request for Review is important and necessary is where the public body has decided to disclose information and a third party objects to that disclosure. In such a case, unless the Request for Review is received within the 30 days, the information will be disclosed at the end of those 30 days and the third party who has failed to request the review within 30 days will be out of luck.

In order to correct this problem, it would be my recommendation that the Information and Privacy Commissioner be given discretion to extend the time for requesting a review in appropriate circumstances, except in the case where the issue is a third party objection to the disclosure of information.

Health Specific Privacy Legislation

The country is charging head long into the era of electronic health records and electronic medical records. Almost every jurisdiction in Canada has now either passed health specific privacy legislation or is developing such legislation to address the very real privacy concerns raised by electronic records. The issues are significant and complicated. What constitutes a use of personal information as opposed to a disclosure? Should there be a "circle of care" model, in which there is implied consent to the use and disclosure of personal information within the circle of care and, if so, what should be included in the circle of care? Who is responsible for the security of personal health information when it crosses territorial/provincial boundaries? Where will the medical health record be stored and how does that affect the security of the system? Should a patient be able to

> Privacy and security are fundamental to electronic health records. With access to complete records, doctors and clinicians will have far better information for decision making. This is especially critical when it comes to prescriptions and treatments that are being provided by multiple doctors or specialists, or when a patient is in an emergency situation.
>
> Excerpt from Canada Health Infoway Web Site

lock away some information so that it can't be accessed by certain medical professionals? What secondary uses of personal health information, if any, should be allowed? These questions represent only the very tip of a very large iceberg of health information issues that will have to be addressed at some point by Nunavut as the whole country moves toward electronic medical and health records. It is time that the Government of Nunavut started to consider these issues with a view to creating health specific privacy legislation to guide us into the era of electronic records.

rules regarding how they gather, use and disclose personal information about individuals. Every jurisdiction in Canada, except for Nunavut, the Northwest Territories, the Yukon, New Brunswick, and Prince Edward Island have legislation which addresses access and privacy at the municipal level.

It has been suggested that no legislation is required for municipalities because the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the federal legislation which governs the protection of personal information in the private sector cov-

In Canada there are 2,000 healthcare transactions every minute.
In one year there are:

- 440 million laboratory tests
- 382 million prescriptions
- 322 million office-based physician visits
- 35 million diagnostic images
- 2.8 million in-patient hospitalizations

Canada Health Infoway Web Site

Municipalities

A recommendation which has been made several times is that municipalities should be subject to access and privacy legislation. Not only is it important that municipal authorities be accountable to the public through access to information rules, it is also important that municipalities have

ers the field. PIPEDA, however, applies only to "commercial activities" and much of what municipalities do would not be considered "commercial activity". Furthermore, PIPEDA does not apply to protect the information of municipal employees. Finally, PIPEDA addresses only privacy issues. It does not address the right of citizens to have access to public records of municipali-

ties. I therefore repeat my recommendation that steps be taken to add municipalities as public bodies under the existing act, or that new legislation be developed to apply to municipal governments in Nunavut.

ance on electronic records and databases is unprecedented. It is estimated that more than 90% of all records being created today are electronic. There is no doubt that the advantages are numerous. We can

> In an age characterized by revolutionary IT developments and exponential information creation, storage, transmission and use, the case for robust and credible information management has never been greater
>
> Ann Cavoukian
> 2007 Annual Report

Electronic Records Management

As more and more reliance is placed on electronic mediums for communication and for storage of records, it becomes more important to ensure that those records are secure, organized and complete. In a paper presented by Sandy Hounsel, the Assistant Information and Privacy Commissioner of Newfoundland and Labrador to the 5th International Conference of Information Commissioners, he made the following observation:

> A crucial aspect of the modern records management system is the explosion over the last number of years of electronic information. The modern workplace has become more and more digital and our reli-

search it, cut and paste it, update it in real time, e-mail it, automate it, audit it, secure it, and control it in ways that paper-based systems simply would not allow. Ultimately, this allows us to work faster, save money and accomplish much more with significantly less effort.

.....

However, organizations often have difficulty cataloguing, organizing and preserving this information, while maintaining a reasonable ability to access it. This is in part due to the failure of many organizations to properly recognize and manage the records management life cycle. This life cycle is equally relevant to both paper records and electronic records, a fact often overlooked by

these organizations. More importantly, however, many organizations appear to be overwhelmed by the volume and variety of electronic records. The technology has simply surpassed the capacity to react appropriately

So many of the reviews which I have conducted in the last number of years involve primarily e-mail records. There is always a concern with such records that they have been properly stored and can be identified as responsive when an application for information is received. Electronic records are only going to increase in volume with time. It is important that the Government of Nunavut keep up with the technologies in terms of its records management system. Perhaps more importantly, it is vital that all government employees working with electronic medium and using the internet to communicate and exchange information completely and fully understand the appropriate rules for storing and recording such transactions and that the records management system that relates to electronic records are clear and strictly enforced. The alternative will result in a complete inability to fully track and account for records created .

Good privacy training of employees is critical to preventing privacy breaches. Human error is one of the most common factors in the cases we investigate. The best privacy policy in the world is of little use if staff doesn't understand it.

Jennifer Stoddart
Privacy Commissioner for Canada

Security of Electronic Medium

As noted in my last Annual Report, there do not seem to be any government wide policies in place with respect to the security of electronic mediums. I could not, for example, find any policy on the use of laptop computers or flash drives and the management of records stored on those devices. Is there a policy on the kinds of data that

can be stored on flash drives and taken out of the office? Are there rules and regulations about the encryption of sensitive data, whether stored on portable devices or on a desktop computer or server? If there are such policies, how well are they known and how well are they enforced?

It is important that there be written government policies regarding electronic medium and that these policies are reviewed regularly to ensure that they keep pace with changing technologies . To the extent that these policies already exist, they should be made part of all orientation programs and should be repeated and reinforced constantly and strenuously enforced with serious consequences attached to a failure to comply with the policies.

Protecting our Children

Today's young people are growing up in an era in which electronic gadgets are the norm. Most of them are far more comfortable with a computer than their parents and the computer, almost by definition these days, includes access to the internet. In a recent press release, the Privacy Commissioner for Canada, Jennifer Stoddart, made the following observation:

> We know children and young people in this country are using the Internet for all sorts of activities – primarily to socialize with their friends. And while the Internet provides a way for our kids to connect with their peers in ways we could have never imag-

---

This case shows how important it is for institutions to keep on top of the proliferation of communications technology and to ensure that employees understand that communications with devices such as BlackBerrys produce records, just like documents, e-mails and voice mails, and that employees have a responsibility to manage them properly.....

However, there is no uniform federal policy on PIN to PIN communication and institutions have been advised to each craft their own policy.

Through our investigation, it became apparent to us that the goals of consistency and simplicity favour a single government policy

Robert Marleau
Information Commissioner for Canada
Annual Report 2007-2008

---

ined a generation ago, we also realize that there are a whole new set of risks that accompany this new medium.

As I read more about the way in which young people use computers, often starting as young as 2 years of age, I have become more concerned about whether or not they, or their parents, fully understand the consequences of some of their activities on line. This generation has grown up with the Internet and they are, therefore, comfortable enough with the medium to experiment, to play with it and on it. They may well recognize the risks associated with their online activities but most often they lack the knowledge to mitigate those risks. Their parents often don't even recognize all the potential risks.

More must be done to educate our young people and provide them with the knowledge they need to protect themselves while they work in the wired world, not only from the obvious risks of pedophiles and identity theft, but also from the less obvious and perhaps more insidious risks that lurk on line. I would recommend that consideration be given to including in school curriculums specific information about electronic medium and strategies for protecting children from on-line risk, beginning at the elementary school level.

We investigated 96 privacy breaches last year. The majority were caused by thefts of computers or vehicles that contained personal information in the form of computers or hard copy files. One public body alone had ten breaches, all involving the same program area and the same risk – workers taking records out of the office and leaving them in a car that was stolen or broken into.
Another large category of breaches involves employee error or misconduct.

David Loukidelis
2007 Annual Report

The Role of the Information and Privacy Commissioner

The workload of the office of Information and Privacy Commissioner is becoming more significant as the public becomes more familiar with the Act and their rights under it. At the moment, the Information and Privacy Commissioner role is filled on a part time "as needed" basis. In past years, the work for this office amounted to an average of about 20 hours each month.

I estimate that in the last eight months, that has been closer to 40 or 50 hours each month. The number of Requests for Review are increasing significantly (although the last year may be an anomaly) and the issues on the privacy side are becoming more and more complex, sometimes requiring significant amount of research and expertise. The "active" role of the Information and Privacy Commissioner is to conduct reviews and make recommendations where there are problems with access to information issues. These have a clear process and anticipated outcome. The time spent on those issues, however, tend to limit the amount of time that can be spent on keeping current with issues on the privacy side of the coin, which involves far more dynamic and shifting issues. Privacy issues require a significant commitment of time to stay abreast of developments but that time is often not available when the position is "part time". It therefore becomes more and more difficult to maintain an appropriate level of expertise on some of the privacy issues. The issues raised by the move toward electronic health and medical records, for example, are very complex and demand specialized background knowledge of medical, technical and technological issues. Nor is there an effective way to ensure that the public education function of the office can be fully realized because of the time commitment necessary to those kinds of activities. It may be that it is time to consider a different approach to the office, perhaps by making it a half time or even a full time position so as to ensure that the Information and Privacy Commissioner has the dedicated time to commit to these other aspects of the job that are otherwise difficult to address. Alternatively, it may be that the Information and Privacy needs to be given a budget to allow her to

> Overall, the theme of the breaches last year was employee error. We have repeatedly reminded organizations and public bodies that ongoing employee training is a critical tool in preventing privacy breaches
>
> David Loukidelis
> 2007 Annual Report

hire contract staff to carry out some of the functions of the office, to assist in investigations or with technical issues or with a public education campaign. The reality is that the time commitment necessary to do an adequate job is growing and eventually it may be necessary to expand the resources dedicated to the office.

The right to be left alone is the beginning of all freedom.

William O. Douglas
U.S. Supreme Court Justice